PCT/EP 99 / 09170

09/856302

4

KONINKRIJK DER NEDERLANDEN

#6
4 Jun 02
R. Talbot

Bureau voor de Industriële Eigendom

EP99/ 91 PO

Hierbij wordt verklaard, dat in Nederland op 20 november 1998 onder nummer 1010616,

ten name van:

PTT POST HOLDINGS B.V.

te Den Haag

een aanvrage om octrooi werd ingediend voor:

"Werkwijze en inrichtingen voor het afdrukken van een frankeerkenmerk op een document",

en dat de hieraan gehechte stukken overeenstemmen met de oorspronkelijk ingediende stukken.

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Rijswijk, 16 september 1999.

De Directeur van het Bureau voor de Industriële Eigendom,
voor deze,
i.o.

mw. I.W. Scheevelenbos - de Reus.

Uittreksel

Werkwijze en inrichtingen voor het afdrukken van een frankeerkenmerk (28) op een document (22) met behulp van de volgende stappen:

a. het beschikbaar stellen van een unieke bitstring;

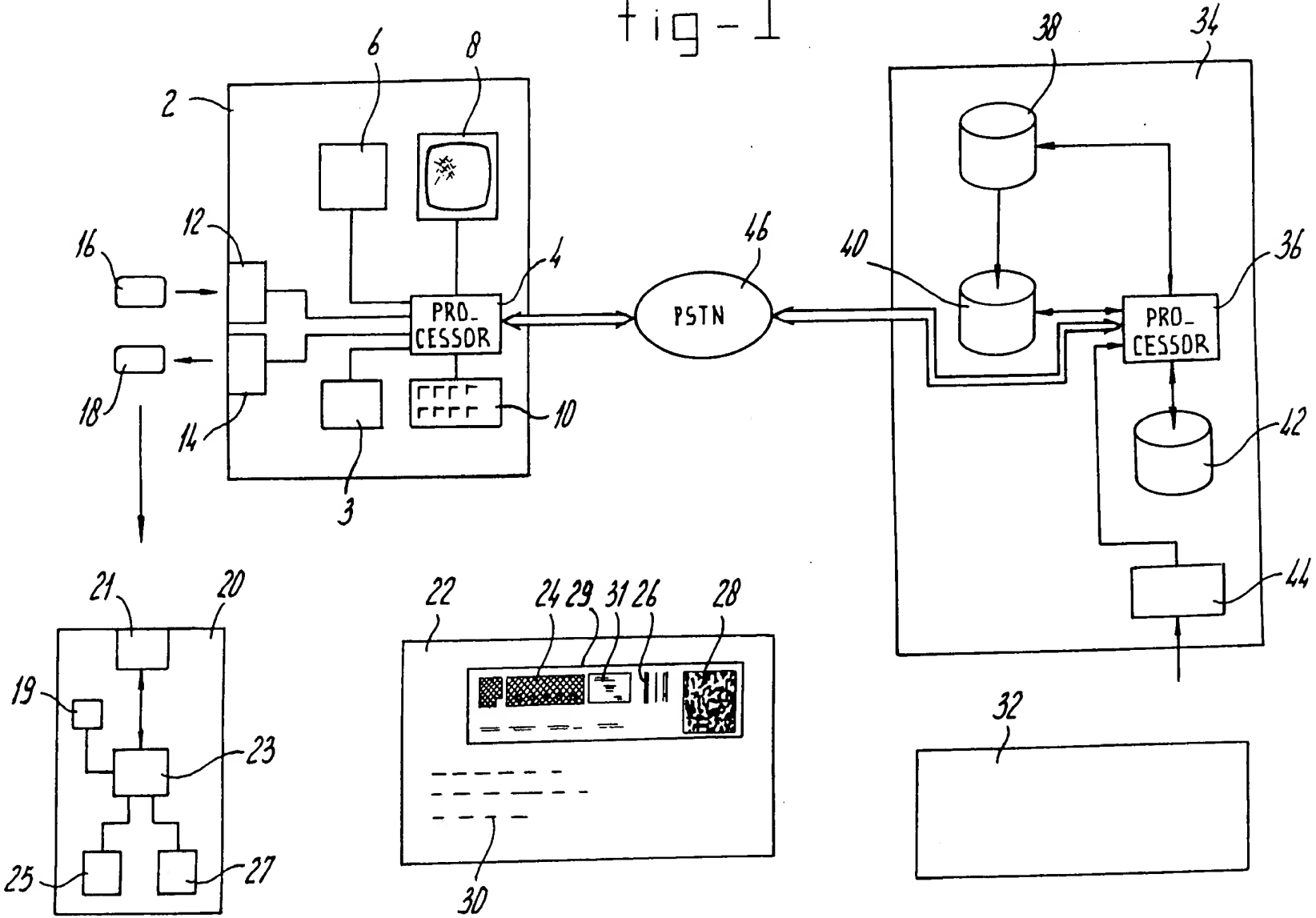
b. het vaststellen van een identificatiecode;

c. het beveiligd afdrukken van het frankeerkenmerk (28) op het document (22), welk frankeerkenmerk tenminste informatie met betrekking tot de bitstring en de identificatiecode omvat;

waarbij de bitstring wordt geselecteerd uit een centraal opgeslagen verzameling van unieke bitstrings en centraal wordt geregistreerd welke unieke bitstrings voor gebruik beschikbaar zijn gesteld.

[fig. 1]

fig-1


2
6
8
12
16
18
14
3
4
PRO-
CESSOR
10
46
PSTN
38
34
40
36
PRO-
CESSOR
42
44
32
21
20
19
23
25
27
22
24
29
31
26
28
30

1010616

Werkwijze en inrichtingen voor het afdrukken van een frankeerkenmerk op een document

De onderhavige uitvinding heeft betrekking op een werkwijze voor het afdrukken van een frankeerkenmerk op een document, omvattende de volgende stappen:

a. het beschikbaar stellen van een unieke bitstring;

b. het vaststellen van een identificatiecode;

c. het beveiligd afdrukken van het frankeerkenmerk op het document, welk frankeerkenmerk tenminste informatie met betrekking tot de bitstring en de identificatiecode omvat.

Met een "frankeerkenmerk" wordt hier bijvoorbeeld verwezen naar een elektronische postzegel, dat wil zeggen een door een frankeermachine of een printer op een poststuk afgedrukt kenmerk, dat onder meer een frankeerwaarde voor het poststuk kan vertegenwoordigen. In het kader van de onderhavige uitvinding heeft "frankeerkenmerk" echter een brede betekenis. Het begrip "frankeerkenmerk" kan naar allerlei typen kenmerken verwijzen die op willekeurige documenten kunnen worden aangebracht ter beveiliging van de documenten. Dergelijke documenten kunnen behalve poststukken ook waardedocumenten zijn, zoals toegangskaarten, betaalbewijzen, enz., die met een dergelijk kenmerk worden beveiligd.

Een werkwijze van de bij de aanvang genoemde soort is bekend uit de volgende twee door Engineering Center voor de United States Postal Service (USPS) openbaar gemaakte documenten: "Information Based Indicia Program (IBIP), Open System Indicium Specification" en "Information Based Indicia Program (IBIP), Open System Postal Security Device (PSD) Specification", beide gedateerd 23 juli 1997 (ontwerpteksten).

Met een dergelijke werkwijze kunnen elektronische postzegels worden verkregen en op poststukken worden afgedrukt. Het apparaat, bijvoorbeeld een computer, waarmee de elektronische postzegel wordt afgedrukt is daartoe voorzien van een Postal Security Device (PSD), waarbij een unieke identificatiecode behoort. De elektronische postzegel omvat diverse elementen, waarvan er enkele als "security critical" worden vermeld: de identificatiecode van de PSD, de waarde van de inhoud van een opklimmend register, de frankeerwaarde van het poststuk en een digitale handtekening. De inhoud van het opklimmende register vertegenwoordigt de totale geldwaarde van alle tot dan toe

1010616

Werkwijze en inrichtingen voor het afdrukken van een frankeerkenmerk op een document

De onderhavige uitvinding heeft betrekking op een werkwijze voor het afdrukken van een frankeerkenmerk op een document, omvattende de volgende stappen:

a. het beschikbaar stellen van een unieke bitstring;

b. het vaststellen van een identificatiecode;

c. het beveiligd afdrukken van het frankeerkenmerk op het document, welk frankeerkenmerk tenminste informatie met betrekking tot de bitstring en de identificatiecode omvat.

Met een "frankeerkenmerk" wordt hier bijvoorbeeld verwezen naar een elektronische postzegel, dat wil zeggen een door een frankeermachine of een printer op een poststuk afgedrukt kenmerk, dat onder meer een frankeerwaarde voor het poststuk kan vertegenwoordigen. In het kader van de onderhavige uitvinding heeft "frankeerkenmerk" echter een brede betekenis. Het begrip "frankeerkenmerk" kan naar allerlei typen kenmerken verwijzen die op willekeurige documenten kunnen worden aangebracht ter beveiliging van de documenten. Dergelijke documenten kunnen behalve poststukken ook waardedocumenten zijn, zoals toegangskaarten, betaalbewijzen, enz., die met een dergelijk kenmerk worden beveiligd.

Een werkwijze van de bij de aanvang genoemde soort is bekend uit de volgende twee door Engineering Center voor de United States Postal Service (USPS) openbaar gemaakte documenten: "Information Based Indicia Program (IBIP), Open System Indicium Specification" en "Information Based Indicia Program (IBIP), Open System Postal Security Device (PSD) Specification", beide gedateerd 23 juli 1997 (ontwerpteksten).

Met een dergelijke werkwijze kunnen elektronische postzegels worden verkregen en op poststukken worden afgedrukt. Het apparaat, bijvoorbeeld een computer, waarmee de elektronische postzegel wordt afgedrukt is daartoe voorzien van een Postal Security Device (PSD), waarbij een unieke identificatiecode behoort. De elektronische postzegel omvat diverse elementen, waarvan er enkele als "security critical" worden vermeld: de identificatiecode van de PSD, de waarde van de inhoud van een opklimmend register, de frankeerwaarde van het poststuk en een digitale handtekening. De inhoud van het opklimmende register vertegenwoordigt de totale geldwaarde van alle tot dan toe

geselecteerd uit een centraal opgeslagen verzameling van unieke bitstrings en centraal wordt geregistreerd welke unieke bitstrings voor gebruik beschikbaar zijn gesteld.

Volgens de uitvinding wordt elke gebruikte unieke bitstring dus centraal gegenereerd en geregistreerd en wordt deze bovendien gekoppeld aan de gebruiker die een elektronische postzegel heeft gekocht en/of de machine die de elektronische postzegels afdrukt. Niet alleen kan dus centraal worden gedetecteerd of de elektronische postzegels slechts een keer worden gebruikt, maar ook fraude makkelijk tot de bron worden herleid. Bovendien kan daardoor eventueel van het gebruik van een PSD worden afgezien.

De werkwijze volgens de uitvinding kan bijvoorbeeld via twee verschillende werkwijzen worden geïmplementeerd.

In een eerste uitvoeringsvorm worden, voorafgaand aan stap c, de unieke bitstring en de identificatiecode, beveiligd met behulp van een eerste message authentication code en/of beveiligd door codering, door een terminal op een informatiedrager met geheugen opgeslagen en geschiedt stap c na inlezing van de informatiedrager door een afdrukeenheid. Een dergelijke informatiedrager kan bijvoorbeeld een chipkaart zijn, waarop meerdere van dergelijke unieke bitstrings tezamen met de identificatiecode kunnen worden opgeslagen. De identificatiecode kan bijvoorbeeld zijn afgeleid uit het nummer van de bank- of giropas van een gebruiker, waarbij de betreffende gebruiker zich heeft geïdentificeerd met behulp van zijn persoonlijk identificatienummer (PIN).

Het is mogelijk dat een dergelijke bankpas of giropas een multifunctionele chipkaart is, bijvoorbeeld een Chipper® van de Nederlandse KPN Telecom en Postbank, die onder meer dienst doet als elektronische beurs. Het is voorts mogelijk dat een dergelijke bankpas/giropas wordt gebruikt voor het direct betalen van de noodzakelijke frankeerwaarde en dat vervolgens dezelfde pas wordt gebruikt als informatiedrager voor het opslaan van de genoemde unieke bitstrings tezamen met de identificatiecode.

Bij voorkeur wordt dan behalve de unieke bitstring en de identificatiecode tevens een terminalidentificatiecode, beveiligd met behulp van de eerste message authentication code en/of door de codering, door de terminal op de informatiedrager met geheugen opgeslagen. In dat geval kan niet alleen de gebruiker op unieke wijze

worden herleid uit het frankeerkenmerk, maar ook de terminal waarbij de gebruiker zijn elektronische postzegels heeft aangeschaft.

Bij voorkeur wordt, na inlezing van de informatiedrager door de afdrukeenheid, gebruik van de unieke bitstring voor afdrukken van een verder frankeerkenmerk op een verder document onmogelijk gemaakt door de afdrukeenheid.

In gevallen waarin een gebruiker grote aantallen frankeerkenmerken op documenten wil afdrukken, kan het onhandig zijn, zo niet fysiek onmogelijk, om op een chipkaart dergelijke grote aantallen unieke bitstrings te moeten opslaan. Het opslaan van grote aantallen bitstrings kan worden vermeden in een uitvoeringsvorm van de uitvinding, waarin bij de unieke bitstring ook de waarde van een teller wordt bijgehouden. De teller bepaalt dan het maximum aantal malen dat de unieke bitstring voor het afdrukken van het frankeerkenmerk op documenten mag worden gebruikt. Als alternatief vertegenwoordigt de teller een saldo voor elektronische postzegels, dat tot de waarde nul mag worden afgeboekt. In dat geval wordt na inlezing van de informatiedrager gecontroleerd of de waarde van de teller op de informatiedrager zich binnen vooraf bepaalde grenzen bevindt. Indien dat het geval is wordt de waarde van de teller na het inlezen aangepast. Zo niet, dan wordt het afdrukken van het frankeerkenmerk geblokkeerd.

In een tweede uitvoeringsvorm van de werkwijze volgens de uitvinding wordt bij het uitvoeren van stap c gebruik gemaakt van een op een (personal) computer aangesloten afdrukeenheid. Bij deze PC uitvoeringsvorm wordt bij voorkeur gebruik gemaakt van een bankpas (smartcard), die via geschikte invoer/uitvoermiddelen met de PC communiceert en feitelijk de functie van een PSD overneemt, die derhalve overbodig is geworden.

Uiteraard kan in deze tweede uitvoeringsvorm ook worden gewerkt met een aan een unieke bitstring toegevoegde teller, die het maximum aantal malen bepaalt dat de unieke bitstring voor het afdrukken van het frankeerkenmerk op documenten mag worden gebruikt of een geldwaarde vertegenwoordigt die aan elektronische postzegels mag worden besteed.

De identificatiecode kan een gebruikersindentificatiecode en/of een afdrukeenheididentificatiecode omvatten. De gebruikersidentificatiecode kan bijvoorbeeld tenminste het nummer van

de bankpas/giropas van de gebruiker inhouden. De afdrukeenheididentificatiecode is bij voorkeur gekoppeld aan een SAM die wordt gebruikt om het frankeerkenmerk beveiligd met een MAC (= message authentication code, ofwel een digitale handtekening) of via codering op het document af te drukken. Deze SAM kan zich in een aparte frankeermachine bevinden, maar ook in een speciaal hiervoor ingerichte (personal) computer.

Bij voorkeur zal het frankeerkenmerk met een tweede message authentication code worden afgedrukt. Tussen deze tweede message authentication code en het frankeerkenmerk bestaat een geheime relatie, die alleen aan de bevoegde autoriteiten bekend zal zijn, waardoor het onmogelijk is om gegevens uit het frankeerkenmerk onopgemerkt te veranderen. Als alternatief kunnen de gegevens ook gecodeerd worden opgeslagen.

Voor het uitvoeren van de werkwijze volgens de uitvinding is de verzameling unieke bitstrings in een eerste centraal geheugen opgeslagen, worden gebruikte combinaties van identificatiecodes en unieke bitstrings in een tweede centraal geheugen opgeslagen, worden op documenten afgedrukte frankeerkenmerken ingelezen, worden in de ingelezen frankeerkenmerken aanwezige combinaties van identificatiecodes en unieke bitstrings in een derde centraal geheugen opgeslagen en worden deze vergeleken met de in het tweede centrale geheugen opgeslagen gebruikte combinaties. Op deze wijze kan precies worden gecontroleerd hoe elke unieke bitstring is gebruikt en kan een gebruiker die eventueel heeft gefraudeerd worden opgespoord. Er kan bijvoorbeeld worden gecontroleerd of elke unieke bitstring slechts eenmaal is gebruikt en niet iemand een frankeerkenmerk heeft gekopieerd.

Voor het uitvoeren van de werkwijze volgens de uitvinding heeft de uitvinding ook betrekking op een systeem voor het afdrukken van een frankeerkenmerk op een document, omvattend:

a. middelen voor het beschikbaar stellen van een unieke bitstring;
b. middelen voor het vaststellen van een identificatiecode;
c. middelen voor het beveiligd afdrukken van het frankeerkenmerk op het document, welk frankeerkenmerk tenminste informatie met betrekking tot de bitstring en de identificatiecode omvat;

met het kenmerk, dat de middelen voor het beschikbaar stellen van de unieke bitstring een eerste centraal opgesteld geheugen met een

verzameling van unieke bitstrings omvatten, waaruit de unieke bitstring wordt geselecteerd, en dat middelen zijn voorzien voor het centraal registreren welke unieke bitstrings voor gebruik beschikbaar zijn gesteld.

Voordelige uitvoeringsvormen van een dergelijk systeem blijken uit de volgconclusies 11 t/m 20.

De onderhavige uitvinding heeft ook betrekking op een centrale voorzien van een eerste centraal geheugen met een verzameling unieke bitstrings, een tweede centraal geheugen voor het opslaan van combinaties van identificatiecodes en verstrekte unieke bitstrings welke combinaties corresponderen met frankeerkenmerken die op een document zijn afgedrukt, centrale invoermiddelen voor het invoeren van op documenten afgedrukte frankeerkenmerken, een derde centraal geheugen voor het opslaan van in de ingevoerde frankeerkenmerken aanwezige combinaties van identificatiecodes en unieke bitstrings en met de centrale invoermiddelen en de eerste, tweede, derde centrale geheugens verbonden processormiddelen voor het met elkaar vergelijken van gegevens in de tweede en derde centrale geheugens.

Voorts heeft de uitvinding betrekking op middelen voor een apparaat dat is ingericht voor het afdrukken van een frankeerkenmerk op een document, welke middelen tenminste zijn ingericht voor het ontvangen van gegevens van een informatiedrager, welke gegevens tenminste een unieke, uit een verzameling van unieke bitstrings afkomstige bitstring omvatten, voor het samenstellen en beschikbaar stellen van gegevens voor het frankeerkenmerk voor het document in beveiligde vorm, zodat het apparaat het frankeerkenmerk beveiligd op het document kan afdrukken, welk frankeerkenmerk tenminste de genoemde gegevens alsmede een identificatiecode omvat. Deze middelen kunnen de vorm hebben van een losse, inbraakvrije module. Als alternatief kunnen zij echter meerdere elementen omvatten die in het betreffende apparaat moeten worden aangebracht.

Bij voorkeur zijn dergelijke middelen ingericht om na ontvangst van de gegevens van de informatiedrager te controleren of de waarde van een teller op de informatiedrager zich binnen voorafbepaalde grenzen bevindt, en indien dit het geval is de informatiedrager te instrueren om de waarde van de teller aan te passen en indien dit niet het geval is het afdrukken van het frankeerkenmerk te blokkeren.

Ook heeft de uitvinding betrekking op een informatiedrager

voorzien van een geheugen met daarin opgenomen tenminste de volgende gegevens: ofwel een unieke, uit een verzameling van unieke bitstrings geselecteerde bitstring, een identificatiecode en een message authentication code die is berekend over tenminste de unieke bitstring en de identificatiecode ofwel de unieke bitstring en de identificatiecode in gecodeerde vorm.

Tenslotte betreft de uitvinding een door een computer uitleesbare informatiedrager, die is voorzien van software, alsmede een gegevensdraaggolf, welke na te zijn ingelezen de computer in staat stelt tot het uitvoeren van een werkwijze voor het afdrukken van een frankeerkenmerk op een document, omvattende de volgende stappen:

a. het ontvangen van een unieke bitstring;
b. het vaststellen van een identificatiecode;
c. het beveiligd afdrukken van het frankeerkenmerk op het document, welk frankeerkenmerk tenminste informatie met betrekking tot de bitstring en de identificatiecode omvat;

waarbij de bitstring wordt ontvangen uit een centraal opgeslagen verzameling van unieke bitstrings.

De onderhavige uitvinding zal hierna worden toegelicht onder verwijzing naar enkele tekeningen, die slechts bedoeld zijn ter illustratie van de uitvinding en niet ter beperking daarvan. In het bijzonder heeft de uitvinding een bredere toepassing dan alleen postverkeer.

Figuur 1 toont een uitvoeringsvorm van een systeem volgens de uitvinding, waarbij gebruik wordt gemaakt van een informatiedrager waarop één of meer elektronische postzegels kunnen worden opgeslagen;

figuur 2a toont de stappen van een werkwijze voor het verstrekken van een elektronische postzegel;

figuur 2b toont de stappen van een werkwijze voor het verschaffen van de elektronische postzegel, waarbij gebruik wordt gemaakt van een teller;

figuur 3a toont de stappen voor het afdrukken van een elektronische postzegel;

figuur 3b toont de stappen voor het afdrukken van een elektronische zegel, waarbij gebruik wordt gemaakt van een teller;

figuren 4a en 4b tonen de stappen van een werkwijze volgens de uitvinding waarbij gebruik wordt gemaakt van een personal computer;

figuur 5 toont een systeem volgens de uitvinding, waarin gebruik

wordt gemaakt van een personal computer.

In figuur 1 verwijst het verwijzingscijfer 2 naar een terminal, die bijvoorbeeld in de muur van een postkantoor is aangebracht. De terminal 2 kan communiceren met een centrale 34, bijvoorbeeld via het public switched telephone network (PSTN) 46. Communicatiewegen via andere netwerken zijn uiteraard mogelijk. Daarbij kan gebruik worden gemaakt van Internet. Communicatie kan ook op andere wijze plaatsvinden, bijvoorbeeld via CDROM's, floppies, enz.

De in figuur 1 getoonde terminal 2 omvat een processor 4, die is gekoppeld met weergeefmiddelen 8 voor het communiceren met een gebruiker. Tevens omvat de terminal 2 een geheugen 6, dat met de processor 4 is verbonden. Met het verwijzingscijfer 10 is schematisch een toetsenbord aangeduid, waarmee een gebruiker gegevens en instructies voor de processor 4 kan invoeren. Daartoe is het toetsenbord 10 verbonden met de processor 4. Verder is de processor 4 verbonden met een Secure Access/Application Module 3 (meestal "SAM" genoemd).

In de in figuur 1 getoonde uitvoeringsvorm is de terminal 2 voorzien van twee invoer/uitvoereenheden 12, 14. In de invoer/uitvoereenheid 12 kan een bankpas of giropas worden ingevoerd. De invoer/uitvoereenheid 12 is daartoe voorzien van een of meer geschikte (niet getoonde) connectoren die met de bankpas en/of giropas 16 in contact kunnen worden gebracht, zoals aan de deskundige bekend is. Met een dergelijke bankpas en/of giropas kan de gebruiker zich zelf identificeren en een PIN-betaling verrichten. In het geval dat deze bankpas/giropas een elektronische beurs bevat, kan de gebruiker hiermee ook betalingshandelingen verrichten, bijvoorbeeld het betalen van een elektronische postzegel die op een poststuk moet worden afgedrukt.

De invoer/uitvoereenheid 14 is ingericht voor het opnemen van een informatiedrager 18, die een chipkaart kan zijn. Daartoe zijn de invoer/uitvoermiddelen 14 voorzien van een of meer geschikte connectoren die met de processor (niet getoond) op de chipkaart 18 contact kunnen maken, zoals aan een deskundige bekend is. Op een dergelijke informatiedrager 18 worden, in een uitvoeringsvorm van de uitvinding, een of meer elektronische postzegels opgeslagen. Dergelijke postzegels worden dan bij voorkeur beveiligd met een message authentication code (MAC) en/of beveiligd door codering

opgeslagen.

In een uitvoeringsvorm is de giropas/bankpas een multifunctionele chipkaart, die onder meer voor betalingsdoeleinden kan worden gebruikt, maar ook ruimte biedt voor andere toepassingen. Een voorbeeld van een dergelijke chipkaart is de Chipper® van de Nederlandse KPN Telecom en Postbank. In dat geval kunnen de kaarten 16 en 18 dezelfde kaart zijn en kunnen de invoer/uitvoermiddelen 12 vervallen.

Als alternatief kan de informatiedrager 18 ook een kaart met bijvoorbeeld een magneetstrip zijn, die zelf niet is voorzien van processormiddelen. In de magneetstrip kunnen dan door de terminal 2 gegevens worden geschreven, gelezen en verwijderd. In dat geval kunnen elektronische postzegels beveiligd door codering worden opgeslagen. Het is denkbaar dat de terminal 2 een voorraad van dergelijke magneetstripkaarten heeft en dat een klant een of meer van dergelijke kaarten koopt. Op de magneetstrip kunnen dan een of meer van dergelijke elektronische postzegels zijn opgeslagen. Dergelijke magneetstripkaarten kunnen wegwerpkaarten zijn. Als wegwerpkaarten kunnen naar keuze ook chipkaarten worden gebruikt.

In figuur 1 verwijst het verwijzingscijfer 20 naar een frankeermachine. De frankeermachine 20 is voorzien van invoer/uitvoermiddelen 21 voor het opnemen van de informatiedrager 18. Tevens is de frankeermachine 20 voorzien van een processor 23, die behalve met de invoer/uitvoermiddelen 21 ook is verbonden met weegmiddelen 25, een drukeenheid 27 en een SAM 19.

Via de invoer/uitvoermiddelen 21 kan de processor 23 communiceren met de informatiedrager 18.

Met behulp van de weegmiddelen 25 kan de frankeermachine 20 het gewicht bepalen van een poststuk 22.

Met behulp van de drukeenheid 27 kan de frankeermachine 20 vervolgens informatie 29 op het poststuk 22 afdrukken.

De informatie 29 omvat bijvoorbeeld voor een mens leesbare gegevens 24 met betrekking tot de postverzendende instantie (of andere reclame), alsmede een merkteken 26 (bijvoorbeeld een streepjescode) voor het automatisch kunnen oriënteren van het poststuk in een stempel/sorteermachine, en een frankeerkenmerk 28 bijvoorbeeld in de vorm van een tweedimensionale streepjescode 28, die verdere, eventueel gecodeerde, informatie bevat. Het frankeerkenmerk 28 zal ten minste

een unieke bitstring inhouden, waarvan het gebruik verderop nog zal worden toegelicht, en een identificatiecode. De identificatiecode identificeert de gebruiker, d.w.z. de persoon die de elektronische postzegel heeft aangeschaft, en/of het apparaat waarmee het frankeerkenmerk wordt afgedrukt. Indien de identificatiecode aan het afdrukapparaat is gekoppeld, kan deze bijvoorbeeld een unieke bij de SAM 19 horende code zijn. In dat geval zal de eigenaar van de frankeermachine verantwoordelijk zijn voor eventuele fraude met het gebruik van elektronische postzegels.

Als identificatiecode van de gebruiker kan het nummer van de bankpas 16 worden gebruikt. Het bankpasnummer is immers een uniek nummer dat gekoppeld is aan de gebruiker, terwijl er een behoorlijke zekerheid kan worden verschaft, dat de gebruiker de eigenaar van de bankpas 16 is, door hem zich te laten identificeren via een PIN-code.

Voorts kan het frankeerkenmerk 28 informatie omvatten met betrekking tot de terminal 2 en de frankeermachine 20, alsmede het type postbezorging (regulier, per expres, aangetekend, per luchtpost, enz.).

Ook kan de frankeerwaarde in een voor een mens leesbare vorm 31 op het poststuk 22 zijn afgedrukt.

Op het poststuk 22 is ruimte ingeruimd voor het adres 30 van de geadresseerde.

Het in figuur 1 getoonde systeem bevat een inrichting 32 om de poststukken 22 tijdens het verzenden van de verzender naar de geadresseerde te kunnen inlezen. Indien de unieke bitstring direct een frankeerwaarde vertegenwoordigt, kan de frankeerwaarde bijvoorbeeld worden gecontroleerd. De door de inrichting 32 ingelezen gegevens worden toegevoerd aan de centrale 34. De informatie die door de inrichting 32 is ingelezen kan op elke bekende wijze aan de centrale 34 worden toegevoerd.

Voor het invoeren van de informatie naar een, in de centrale 34 aanwezige processor 36 is de centrale 34 voorzien van geschikte invoermiddelen 44, die met de processor 36 zijn verbonden.

Voor het uitvoeren van de werkwijze volgens de uitvinding is de centrale 34 bij voorkeur voorzien van drie geheugens 38, 40, 42. Dit hoeven uiteraard geen fysiek gescheiden geheugens te zijn. Zij kunnen verwijzen naar verschillende velden binnen één groter geheugen.

Figuur 2a geeft een mogelijke uitvoeringsvorm weer van de

werking van de terminal 2 tijdens bedrijf.

Een klant komt bij de terminal 2 en stopt zijn bankpas 16 (hiermee zal in het vervolg zowel een bankpas/giropas of elke (multifunctionele) chipkaart worden bedoeld) in de overeenkomstige invoer/uitvoermiddelen 12. De processor 4 vraagt via de monitor 8 welk type elektronische postzegels de klant wenst te hebben. De klant kan bijvoorbeeld aangeven dat hij een frankeerpas 18 (deze benaming zal vanaf hier worden gebruikt voor elk mogelijk type informatiedrager 18) met 100 elektronische postzegels van 80 cent wil kopen. Dit gebeurt in stap 202.

De processor 4 leest het nummer van de bankpas 16 in en vraagt de gebruiker zich te identificeren met zijn PIN-code, stappen 204 en 206.

In stap 208 controleert de processor 4 op op zichzelf bekende wijze of de klant zich correct heeft geïdentificeerd. Zo niet, dan volgt een foutmelding in stap 210. Na de foutmelding in stap 210 kan de processor 4 terugkeren naar het begin van het stroomschema dat in figuur 2a is getekend. Als alternatief kan een gebruiker, zoals op zichzelf bekend is, drie keer de mogelijkheid krijgen om de correcte PIN-code in te voeren.

Heeft een gebruiker zich op de correcte wijze geïdentificeerd, dan springt het programma in de processor 4 naar stap 212 en leest het een frankeernummer in. In overeenstemming met de uitvinding bestaat het frankeernummer uit een bitstring die uniek is en is gekozen uit een verzameling van unieke bitstrings.

De verzameling van unieke bitstrings is opgeslagen in het geheugen 38 in de centrale 34. Deze centrale 34 is met meerdere over het land verspreide terminals 2 verbonden en kan, bijvoorbeeld via het PSTN 46, één of meer unieke frankeernummers uit de verzameling unieke frankeernummers beschikbaar stellen voor de terminals 2. Daarbij kan per transactie een bepaalde hoeveelheid gewenste unieke frankeernummers uit het geheugen 38 in de centrale 34 naar het geheugen 6 in de terminal 2 worden overgedragen. Als alternatief kan ieder van de terminals 2 echter een bepaalde voorraad unieke frankeernummers vooraf in het geheugen 6 hebben opgeslagen, zodat niet iedere keer bij een transactie met een klant een verbinding tussen de terminal 2 en de centrale 34 hoeft te worden gelegd. Transmissie van de unieke bitstrings kan beveiligd op elke bekende wijze plaatsvinden.

De verzameling unieke frankeernummers in het geheugen 38 van de centrale 34 bestaat bijvoorbeeld uit bitstrings van 128 bits. Aldus bevat deze verzameling een zodanig groot aantal unieke frankeernummers, dat de behoefte aan dergelijke nummers jarenlang zal zijn gedekt.

Bij voorkeur voorafgaand aan stap 212 betaalt de klant de frankeerpas 18 op elektronische wijze. Dit gebeurt op op zichzelf bekende wijze met behulp van de bankpas 16. Dat wil zeggen dat als de bankpas 16 een reguliere bankpas is, de betaling plaatsvindt door afboeking van het banksaldo van de klant. De wijze waarop dit gebeurt is aan de deskundige bekend en behoeft hier geen verdere toelichting. In het geval dat de bankpas 16 een elektronische beurs omvat, kan het verschuldigde bedrag direct van het saldo van de bankpas 16 worden afgeboekt. Betaling kan ook contant plaatsvinden.

De processor 4 verschaft dan via de invoer/uitvoermiddelen 14 een aparte frankeerpas 18 waarop zowel de identificatiecode als de betreffende frankeernummers zijn opgeslagen. In een uitvoeringsvorm zijn deze identificatiecode en deze frankeernummers opgeslagen met een message authentication code MAC1, die door de SAM 3 van de terminal 2 tezamen met de processor van de bankpas 16 wordt berekend. Zoals bekend is een MAC een checksum van aangeboden tekst, waarmee kan worden gecontroleerd of de aangeboden tekst valide is. Elke wijziging in de tekst (in dit geval de identificatiecode en de frankeernummers) kan worden waargenomen. Een MAC is alleen na te rekenen met een geheime sleutel, die alleen aan de SAM 3 en de bevoegde postautoriteiten bekend is. Het genereren van MAC1 en het opslaan van de nodige gegevens op de frankeerpas 18 vindt plaats in de stappen 214 en 216.

Als alternatief voor het berekenen van een MAC kunnen de gegevens ook gecodeerd worden opgeslagen.

Ter verdere beveiliging van het geheel stuurt de processor 4 bij voorkeur een kopie van de identificatiecode met de uitgegeven frankeernummers beveiligd met MAC1 en/of beveiligd door codering naar de centrale 34, die deze informatie opslaat in geheugen 40, zodat in een later stadium centraal eventuele fraude kan worden gecontroleerd, stap 218. Hierop zal hierna nog worden ingegaan.

In het geheugen van de frankeerpas 18 kan naar wens een terminalcode zijn opgeslagen, die op unieke wijze de terminal 2

identificeert, die de frankeerpas 18 heeft uitgegeven. Naar wens kan deze terminalcode onderdeel uitmaken van de berekening die MAC1 heeft opgeleverd. Dan kan namelijk ook de terminalcode niet onopgemerkt worden gewijzigd.

Figuur 3a toont een stroomdiagram van de werking van een frankeermachine 20 in overeenstemming met de werkwijze zoals toegelicht onder verwijzing naar figuur 2a.

Een gebruiker steekt zijn frankeerpas 18 in de daartoe bestemde invoer/uitvoermiddelen 21 van de frankeermachine 20. Daarmee wordt een contact tot stand gebracht tussen de frankeerpas 18 en de processor 23 van de frankeermachine 20. De gebruiker geeft via geschikte invoermiddelen (bijvoorbeeld een niet getoond toetsenbord) de processor 23 opdracht om een elektronische postzegel op poststuk 22 af te drukken. Zodra de processor 23 heeft vastgesteld, dat een dergelijke instructie is ontvangen, stap 302, leest de processor 23 ofwel MAC1 met bijbehorende identificatiecode en frankeernummer ofwel de identificatiecode en het frankeernummer in gecodeerde vorm in van de frankeerpas 18. Indien aanwezig zal ook de terminalcode, die in de frankeerpas 18 is opgeslagen, worden ingelezen.

Op basis van de ingelezen gegevens stelt de frankeermachine 20 op vooraf bepaalde wijze een frankeerkenmerk samen en drukt dit af op het poststuk 22, stap 306. Daartoe is de frankeermachine 20 op op zichzelf bekende wijze voorzien van een opening waarin het poststuk 22 kan worden gestoken, zodat met behulp van de drukeenheid 27 het frankeerkenmerk op het poststuk 22 kan worden afgedrukt.

Het kan bijvoorbeeld zo zijn dat de processor 23 in staat is om te controleren of de frankeerwaarde genoeg is gezien het gewicht van het poststuk 22. Daartoe wordt het poststuk 22 gewogen met de weegmiddelen 25, die een weegsignaal naar de processor 23 sturen. Het frankeernummer kan bijvoorbeeld tot een bepaalde subgroep van alle unieke frankeernummers behoren, die alleen voor poststukken tot en met 50 gram mogen worden gebruikt. Per gewichtsklasse en per type postbezorging is dan een aparte subgroep unieke frankeernummers beschikbaar. Aldus kan de processor 23 direct controleren of de frankeerwaarde correct is en, indien dit niet het geval is, de gebruiker waarschuwen via een (niet weergegeven) display.

Het frankeerkenmerk wordt bijvoorbeeld in de vorm van een tweedimensionale streepjescode 28 op het poststuk 22 afgedrukt. Bij

voorkeur omvat het frankeerkenmerk tenminste de volgende gegevens: het betreffende frankeernummer, de identificatiecode van de gebruiker, de terminalcode van de terminal 2, en een frankeermachinecode die de frankeermachine 20 identificeert. Bij voorkeur worden deze gegevens voorzien van een verdere MAC (MAC2) in het frankeerkenmerk afgedrukt. Een dergelijke MAC 2 wordt berekend door SAM 19 in de frankeermachine 20 tezamen met de frankeerpas 18, die daarvoor van een processor (niet getoond) moet zijn voorzien. Als alternatief kunnen de gegevens ook in gecodeerde vorm worden afgedrukt, waarbij de codering met behulp van bekende cryptografische technieken (waaronder eventueel het plaatsen van een digitale handtekening) plaatsvindt.

Naar keuze kan het frankeerkenmerk 28 ook omvatten: adresinformatie van geadresseerde en verzender (eventueel retouradres), service-informatie zoals "aangetekend", "per expres", enz., en datum en tijd. Deze informatie kan dan met de bovengenoemde gegevens gecodeerd worden met behulp van bekende cryptografische technieken.

Nadat de frankeermachine 20 het frankeerkenmerk op het poststuk 22 heeft afgedrukt, kan de frankeermachine 20 elk volgend gebruik van het gebruikte frankeernummer op de frankeerpas 18 onmogelijk maken. Dit gebeurt in stap 308. Dit kan bijvoorbeeld gebeuren door het betreffende frankeernummer op de frankeerpas 18 te verwijderen.

Bij verzending van het poststuk 22 van een verzender naar een ontvanger, zal het poststuk 22 op een gegeven moment in een distributiecentrum terecht komen. Daar zal het poststuk 22 met behulp van de middelen 32 worden ingelezen en kan nogmaals worden gecontroleerd of het poststuk 22 voldoende gefrankeerd is. De middelen 32 lezen ten minste het frankeerkenmerk 28 in. De middelen 32 verzamelen aldus alle ingelezen frankeerkenmerken 28 van alle poststukken, die daarvan zijn voorzien. Alle frankeerkenmerken 28 worden vervolgens verzonden naar de centrale 34 en daar door de processor 36 via de invoermiddelen 44 ingelezen. De processor 36 slaat de ingevoerde frankeerkenmerken op in het geheugen 42.

De processor 36 had in een eerder stadium reeds gegevens van de terminals 2 ontvangen met betrekking tot ofwel uitgegeven frankeernummers met bijbehorende identificatiecodes en MAC1's ofwel gecodeerde frankeernummers met bijbehorende identificatiecodes. Deze gegevens werden door de processor 36 in het geheugen 40 opgeslagen.

Aldus is de processor 36 in staat om de via de invoermiddelen 44 ontvangen gegevens, na opslag in het geheugen 42, te vergelijken met de in het geheugen 40 opgeslagen gegevens. Aldus kan worden gecontroleerd of de in het geheugen 42 aanwezige frankeernummers inderdaad zijn uitgegeven. Indien er op enige wijze is geknoeid met het frankeernummer, de identificatiecode, de terminalcode en/of de frankeermachinecode, dan kan de processor 36 dit direct afleiden uit de in het frankeerkenmerk opgenomen MAC1 en MAC2 of gecodeerde gegevens. Bovendien kan de processor 36 dan herleiden bij welke terminal 2 en/of welke gebruiker onregelmatigheden hebben plaatsgevonden. De identificatiecode identificeert immers de gebruiker en/of de SAM 3 in de terminal 2 op unieke wijze.

Een verdere controle vindt plaats doordat de processor 36 bijhoudt welke unieke frankeernummers naar de terminals 2 zijn verzonden, bijvoorbeeld door deze frankeernummers op te slaan in het geheugen 40. Uiteraard kunnen deze frankeernummers ook in een ander geheugen worden opgeslagen. Ten eerste kunnen deze reeds naar de terminals 2 verzonden frankeernummers dan niet nog een keer worden verzonden. Ten tweede kunnen de door de terminals 2 naar de centrale 34 verzonden gegevens dan reeds in een eerste ronde met de uitgegeven frankeernummers worden vergeleken, zodat direct kan worden gecontroleerd of de door de terminals 2 uitgegeven frankeernummers inderdaad frankeernummers zijn, die vanuit het geheugen 38 zijn verzonden.

Als het frankeerkenmerk 28 een identificatiecode bezit die de eigenaar van de bankpas 16 op unieke wijze identificeert, is het mogelijk om de uitvinding uit te voeren met betaling achteraf. De processor 36 kan dan immers uit de ontvangen frankeerkenmerken 28 op eenduidige wijze afleiden welke klanten welke frankeernummers hebben gebruikt. Dit opent de mogelijkheid, dat de middelen 32 bijvoorbeeld het gewicht van het poststuk 22 meten en het gewicht tezamen met het frankeerkenmerk 28 meedelen aan de processor 36. De processor 36 stelt in dat geval op dat moment vast hoeveel de klant voor het versturen van het betreffende poststuk moet betalen, een en ander afhankelijk van bijvoorbeeld het gewicht van het poststuk 22 en het type van verzending. Het betreffende bedrag wordt dan op op zichzelf bekende wijze afgeboekt van het saldo van de klant bij de bank. Uiteraard kan in plaats daarvan een factuur worden gestuurd of het saldo worden

afgeboekt bij een andere bank, waarmee op op zichzelf bekende wijze een communicatieverbinding tot stand wordt gebracht. Het voordeel van deze alternatieve methode is, dat het uitgeven van frankeernummers nog niet gekoppeld is aan de waarde die nodig is gezien het gewicht en het type van verzending van het poststuk 22. Het unieke frankeernummer is dan slechts een identificatie van het poststuk 22. Het frankeernummer hoeft dan geen informatie met betrekking tot de frankeerwaarde te omvatten.

In theorie zijn er dus twee typen kaarten mogelijk: oplaadbare kaarten (bijvoorbeeld chipkaarten) en niet-oplaadbare kaarten (bijvoorbeeld magneetstripkaarten). Verder zijn in theorie in beide gevallen drie verschillende manieren van betaling mogelijk: geheel vooraf betalen van elke elektronische postzegel, geheel achteraf betalen van elke elektronische postzegel, en een combinatie van vooraf betaalde en achteraf te betalen elektronische postzegels.

Figuren 2b en 3b tonen stroomdiagrammen voor een alternatieve uitvoeringsvorm van de werkwijze volgens de uitvinding. Deze alternatieve werkwijze heeft betrekking op een uitvoeringsvorm, waarin niet per poststuk een uniek frankeernummer wordt toegepast. In sommige gevallen zou een klant bijvoorbeeld 1000 of meer poststukken willen frankeren. Met de op dit moment beschikbare middelen voor opslag van gegevens op creditkaarten en/of van magneetstrippen voorziene kaarten is het onmogelijk om dergelijke grote aantallen unieke frankeernummers, bijvoorbeeld bestaande uit 128 bits, op te slaan. Dit probleem kan worden ondervangen door een frankeernummer met een bepaalde tellerstand te verschaffen.

De werkwijze voor het verschaffen van een elektronische zegel met teller wordt toegelicht aan de hand van figuur 2b. Stap 252 correspondeert met stap 202 uit figuur 2a.

Stap 254 geeft op verkorte wijze weer dat een gebruiker zich moet identificeren, bijvoorbeeld op de wijze zoals is toegelicht aan de hand van stappen 204-210 in figuur 2a.

Stap 256 correspondeert met stap 212 uit figuur 2a.

Nadat de processor 4 het frankeernummer heeft ingelezen, stelt de processor 4 in stap 258 een tellerstand in. Dit kan de processor 4 bijvoorbeeld doen door de gebruiker via de monitor 8 te vragen om een dergelijke tellerstand op te geven. De hoogte van de tellerstand bepaalt dan het aantal malen dat het betreffende frankeernummer mag

worden gebruikt. Als alternatief kan de teller een geldwaarde vertegenwoordigen die aan elektronische postzegels mag worden besteed. De tellerstand kan de gebruiker via de toetsen van het toetsenbord 10 invoeren.

In stap 260 genereert de processor 4 MAC1 over de identificatiecode van de gebruiker, het uitgegeven frankeernummer en de tellerstand. Deze gegevens kunnen als alternatief gecodeerd worden opgeslagen. De tellerstand is dan dus ook beveiligd opgeslagen en kan niet onopgemerkt worden gewijzigd.

In stap 262 slaat de processor 4 ofwel MAC1 met de identificatiecode, het uitgegeven frankeernummer en de tellerstand ofwel de gecodeerde gegevens op op de frankeerpas 18.

De frankeerpas 18 kan weer elke uitvoeringsvorm hebben zoals hierboven is toegelicht onder verwijzing naar figuur 2a.

In stap 264 stuurt de processor 4 een kopie van MAC1 met identificatiecode, frankeernummer en tellerstand of de gecodeerde vorm van deze gegevens naar de centrale 34. De centrale 34 slaat de gegevens weer op in het geheugen 40 en dus weet deze hoe vaak het betreffende frankeernummer mag worden gebruikt.

Figuur 3b toont een stroomschema van de werking van frankeermachine 20 voor de uitvoeringsvorm waarin gebruik wordt gemaakt van een teller.

In stap 352 wacht de frankeermachine 20 totdat de klant een verzoek tot het afdrukken van een elektronische postzegel heeft gedaan. Deze stap komt overeen met stap 302 uit figuur 3a.

Zodra de klant dit verzoek heeft gedaan, leest de frankeermachine ofwel MAC1 met identificatiecode, frankeernummer en tellerstand ofwel deze gegevens in gecodeerde vorm in van de frankeerpas 18. Dit gebeurt in stap 354.

In stap 356 controleert de processor 23 of de ingelezen tellerstand nog groter dan nul is. Is dit niet het geval, dan mag het betreffende frankeernummer niet meer worden gebruikt en volgt er een foutmelding in stap 358. Het programma keert na stap 358 terug naar stap 352.

Is de tellerstand wel groter dan nul, dan gaat het programma van de processor 23 door met stap 360. In stap 360 bestuurt de processor 23 de drukeenheid 27 zodanig, dat het frankeerkenmerk, dat door de processor 23 is berekend, wordt afgedrukt op het poststuk 22. Opnieuw

wordt bij voorkeur dit frankeerkenmerk voorzien van MAC2. Als alternatief worden alle gegevens gecodeerd in het frankeerkenmerk afgedrukt.

Daarna verlaagt de processor 23 in stap 362 de tellerstand op de frankeerpas 18 om aan te geven, dat het betreffende unieke frankeernummer een keer minder gebruikt mag worden, of om de beschikbare waarde te verlagen.

Uiteraard houdt de berekening van MAC2 ook rekening met de gewijzigde tellerstand.

De actuele tellerstand maakt dan onderdeel uit van het frankeerkenmerk 28 op het poststuk 22.

Opgemerkt wordt, dat de combinatie van uniek frankeernummer en actuele tellerstand dan nog steeds een unieke bitstring inhoudt. Deze laatste bitstring heeft dan alleen meer bits dan het aantal bits van het unieke frankeernummer.

De actuele tellerstand wordt dan meegelezen door de middelen 32 en vervolgens ook via de invoermiddelen 44 met behulp van de processor 36 in de centrale 34 opgeslagen in het geheugen 42. De processor 36 heeft dan de mogelijkheid om te controleren of elke combinatie van frankeernummer en tellerstand inderdaad slechts eenmaal wordt gebruikt. Aangezien de betreffende informatie beveiligd door MAC2 of beveiligd door codering is opgeslagen, is ongeoorloofde wijziging van deze getallen door de processor 36 te detecteren.

De processor 36 kan tevens controleren of de klant het frankeernummer het toegelaten aantal malen heeft gebruikt.

Het zal duidelijk zijn dat de uitvoeringsvorm volgens figuren 2b en 3b, net als de uitvoeringsvorm volgens figuren 2a en 3a, kan worden gebruikt met betaling vooraf en betaling achteraf.

Optioneel is het mogelijk om in de uitvoeringsvorm volgens figuur 1, waar gebruik wordt gemaakt van de frankeerpas 18, het gebruik van de frankeerpas 18 te beperken tot een van tevoren geselecteerd aantal frankeermachines 20. Daartoe kunnen de frankeerpassen 18 worden voorzien van die frankeermachinecodes behorend bij die frankeermachines 20, waarop gebruik van de frankeerpas 18 geoorloofd is.

Een verdere optie is om het in figuur 1 getoonde systeem zodanig uit te voeren, dat ieder van de frankeerpassen 18 ook een uniek nummer krijgt toegewezen. Dan is het mogelijk om eventuele fraude met

frankeerpassen 18 te lokaliseren. Het is dan mogelijk om op een willekeurige frankeerpas 18 informatie op te laten nemen met betrekking tot die frankeerpassen 18 waarmee wordt gefraudeerd. Deze informatie met betrekking tot de frankeerpassen 18 waarmee wordt gefraudeerd, kan dan "onder water" worden overgedragen naar de frankeermachines 20, die de betreffende informatie in een (niet getoond) geheugen opslaan. Als dan een klant met een frankeerpas 18 waarmee wordt gefraudeerd een elektronische postzegel wenst af te drukken, kan de frankeermachine 20 de betreffende frankeerpas 18 detecteren en deze ongeldig maken. Dit kan gebeuren door ofwel de inhoud van de frankeerpas 18 te wissen of onleesbaar te maken, ofwel eenvoudig het afdrukken van een elektronische postzegel te weigeren. Daarmee kan verdere schade door eventuele fraude worden verminderd.

Als alternatief voor het gebruik van een teller kan ook worden gewerkt met een frankeernummer, dat bijvoorbeeld een vooraf bepaald aantal dagen door de klant mag worden gebruikt. Dit kan alleen in de uitvoeringsvorm waarmee betaling achteraf plaatsvindt. In dat geval is het frankeernummer nog steeds uniek, maar wordt het frankeernummer voor meer dan één poststuk 22 gebruikt. Omdat in dat geval een frankeerpas 18 met een bepaald uniek frankeernummer een niet vooraf bepaald aantal malen kan worden gebruikt, verdient het de voorkeur in een dergelijke uitvoeringsvorm het gebruik van een PIN-code toe te passen, die de gebruiker van de frankeerpas 18 nodig heeft om de frankeerpas 18 bij de frankeermachine 20 te kunnen gebruiken. In dat geval moet de frankeermachine 20 zodanig zijn ingericht, dat deze de bij de frankeerpas 18 behorende PIN-code kan controleren.

Figuur 5 toont een alternatieve uitvoeringsvorm van de uitvinding, waarin gebruik wordt gemaakt van een PC van een gebruiker in plaats van een terminal 2 zoals in figuur 1 is getoond.

Onderdelen die hetzelfde zijn in figuren 1 en 5 hebben dezelfde verwijzingscijfers.

In figuur 5 verwijst verwijzingscijfer 52 naar de microprocessor van de PC 50 van een gebruiker. De microprocessor 52 is verbonden met een monitor 54, een printer 62, een toetsenbord 58 en, indien gewenst, een muis 60. In één uitvoeringsvorm is de microprocessor ook verbonden met invoer/uitvoermiddelen 14, die een bankpas 18 (multifunctionele chipcard) kunnen opnemen. Voor het berekenen van MAC's of het bepalen van coderingen van de af te drukken gegevens kan de microprocessor 52

gekoppeld zijn aan een SAM 64.

De microprocessor 52 is, bijvoorbeeld via het PSTN, verbonden met een server systeem 70, waarop meerdere computersystemen kunnen zijn aangesloten. Er kunnen meerdere server systemen zijn voorzien, ieder met hun eigen aansluitingen naar PC's. Het server systeem 70 is met de centrale 34 verbonden. Het server systeem 70 omvat een server processor 72, waarmee een SAM of HSM (= Host Security Module = een computersysteem met dezelfde functionaliteit als een SAM, maar met veel grotere capaciteit) 74 is verbonden.

Het communiceren tussen de PC 50 en het server systeem 70 kan bijvoorbeeld plaatsvinden met een internet protocol (IP).

Figuur 4a toont een stroomschema van een uitvoeringsvorm van de werking van de PC 50 in het kader van de onderhavige uitvinding voor het opladen van een bankpas 18 met een bepaald gewenst saldo, dat aan elektronische zegels kan worden besteedt. Figuur 4b betreft het daadwerkelijk afdrukken van een dergelijke elektronische zegel met een dergelijke bankpas 18.

In stap 402 wacht de microprocessor 52 totdat een gebruiker een verzoek tot het verschaffen van een saldo voor één of meer elektronische postzegels heeft gedaan. Voor het uitvoeren van een dergelijk verzoek, maakt de gebruiker gebruik van de bekende invoermiddelen, zoals toetsenbord 58 en/of muis 60. Daarbij steekt de gebruiker eerst zijn bankpas 18 in de invoer/uitvoereenheid 14.

Daarna vraagt de microprocessor 52 via de monitor 54 of de gebruiker zich op unieke wijze wil identificeren, stap 404. Dit kan bijvoorbeeld gebeuren doordat de gebruiker zijn bankpas 18 in de invoer/uitvoermiddelen 14 steekt, zodat de microprocessor 52 het nummer van de bankpas 18 kan lezen. Vervolgens zal de gebruiker zich, bijvoorbeeld met behulp van een PIN-code, moeten identificeren om duidelijk te maken dat hij de gerechtigde gebruiker van de bankpas 18 is. Controle van de PIN-code geschiedt, zoals bekend, bij voorkeur op de bankpas 18 zelf. Vervolgens kan de microprocessor 52 er van uitgaan dat de gebruiker op unieke wijze is geïdentificeerd met behulp van bijvoorbeeld het bankpasnummer. Dit gebeurt in stap 404. Als alternatief kan de microprocessor 52 de gebruiker vragen de combinatie van bankpasnummer en PIN of een andere unieke combinatie via toetsenbord 58 in te voeren, waarna deze gegevens lokaal door de PC 50 worden gecontroleerd. De PC 50 moet deze combinatie van gegevens dan

wel beveiligd hebben opgeslagen.

In stap 406 vraagt de microprocessor een uniek frankeernummer op bij de centrale 34. Dit gebeurt op eenzelfde wijze als hiervoor is toegelicht onder verwijzing naar de figuren 2a en 2b.

Vervolgens genereert de SAM 74 van het server systeem 70 tezamen met de bankpas 18 een MAC, MAC1, over de identificatiecode van de gebruiker, het betreffende frankeernummer en het saldo dat voor elektronische zegels beschikbaar is gesteld. Als alternatief berekent het server systeem 70 een codering van de identificatiecode, het frankeernummer en het genoemde saldo. Dit gebeurt in stap 408.

In stap 410 slaat de microprocessor naar keuze MAC1, de identificatiecode, het frankeernummer en het genoemde saldo op op de bankpas 18. Als in plaats van een MAC-berekening een coderingsstap heeft plaatsgevonden, worden de coderingen van de identificatiecode, het frankeernummer en het genoemde saldo op de bankpas opgeslagen.

In stap 412 stuurt het serversysteem 70 een kopie van ofwel MAC1, de identificatiecode, het frankeernummer en het saldo ofwel de coderingen van de identificatiecode, het frankeernummer en het saldo naar de centrale 34. De centrale 34 zal deze gegevens weer opslaan in zijn geheugen 40.

Na stap 412 is de opslag van een saldo op de bankpas 18, dat is te gebruiken voor elektronische zegels, afgerond.

Figuur 4b toont hoe een gebruiker met zijn aldus van een saldo voorziene bankpas 18 de PC 50 kan instrueren om een frankeerkenmerk op een poststuk te printen.

Nadat het desbetreffende programma is gestart, stap 450, wacht de PC 50 totdat de gebruiker een verzoek tot het afdrukken van een frankeerkenmerk heeft gedaan, stap 452.

Via stap 454 ervaart de PC 50 hoe hoog de portokosten zijn die in het frankeerkenmerk moeten worden verwerkt. De gebruiker kan de portokosten bijvoorbeeld via het toetsenbord 58 invoeren. Het is denkbaar deze stap te automatiseren met behulp van een met de PC 50 verbonden, automatische weegschaal (niet getoond) die het poststuk weegt, waarna automatisch de portokosten worden bepaald en aan de PC 50 worden doorgegeven.

De gebruiker heeft zijn bankpas 18 weer in contact gebracht met de invoer/uitvoermiddelen 14 en zich weer geïdentificeerd met behulp van zijn PIN-code. De microprocessor 52 leest MAC1, de

identificatiecode, het frankeernummer en het actuele saldo van de bankpas 18, stap 456.

De microprocessor 52 controleert vervolgens, stap 458, of het actuele saldo voldoende is voor de gewenste portokosten. Zo niet, dan volgt in stap 460 een melding aan de gebruiker, die bijvoorbeeld inhoudt dat de gebruiker zijn saldo op de bankpas moet bijladen.

In stap 462 instrueert de microprocessor 52 de printer 62 tot het afdrukken van een frankeerkenmerk, dat door de SAM 64 is berekend, op het poststuk 22 nadat de gebruiker het poststuk 22 in de printer 62 heeft ingevoerd. Daarbij berekent SAM 64 samen met de bankpas 18 MAC2 over alle gegevens die in het frankeerkenmerk zijn opgenomen, waaronder: de identificatiecode, het unieke frankeernummer, het actuele saldo en de portokosten. Als alternatief voor het berekenen van een tweede MAC, MAC2, kunnen deze gegevens gecodeerd worden. Tot de gegevens behoort bij voorkeur ook een PC-code die de PC 50 op unieke wijze identificeert.

Na stap 462 wordt in stap 464 het actuele saldo verlaagd door daarvan de portokosten af te trekken. Het nieuwe actuele saldo vertegenwoordigt dan het bedrag dat nog voor verdere elektronische zegels beschikbaar is.

Opgemerkt wordt dat bij de uitvoeringsvorm die aan de hand van figuren 4a, 4b en 5 is beschreven een uniek frankeernummer net zolang gebruikt wordt totdat het oorspronkelijke saldo is verbruikt. Omdat in elk frankeerkenmerk echter ook het actuele saldo en de actuele portokosten zijn opgenomen is er echter per poststuk nog steeds sprake van een unieke bitstring.

Na stap 464 keert het programma terug naar stap 450.

Bij voorkeur vindt de betaling door de klant direct plaats op het moment dat de klant het saldo op zijn bankpas bijlaadt. Dit kan op op zichzelf bekende wijze langs elektronische weg plaatsvinden. De afboeking kan daarbij weer plaatsvinden via de centrale 34 van een centraal banksaldo of direct van de bankpas 18 als deze een elektronische beurs omvat.

Het is echter eveneens denkbaar om betaling achteraf te laten plaatsvinden, zoals hiervoor is toegelicht onder verwijzing naar de uitvoeringsvorm van figuur 1. Daarbij vertegenwoordigt het op de bankpas 18 geladen saldo niet een totaalbedrag dat aan elektronische zegels kan worden besteed, maar het aantal malen, dat het verstrekte

frankeernummer kan worden gebruikt. Het voordeel van betaling achteraf is, dat de gebruiker niet vooraf zijn poststuk 22 hoeft te wegen om de juiste frankeerwaarde in het frankeerkenmerk 28 aanwezig te laten zijn. Ook hier identificeert het frankeerkenmerk immers op unieke wijze de gebruiker, die vervolgens de rekening kan krijgen toegestuurd of van wie op automatische wijze afboeking van zijn banksaldo kan plaatsvinden. Bovendien garandeert de aanwezigheid van het unieke frankeernummer met identificatiecode, en het actuele "saldo", dat elk poststuk 22 op unieke wijze is geïdentificeerd, zodat fraude direct kan worden opgemerkt.

Verder wordt opgemerkt, dat het mogelijk is om in plaats van of samen met een identificatie van de gebruiker een identificatie van de SAM 64 in het frankeerkenmerk te verwerken. In dat geval is de eigenaar van de PC 50 met SAM 64 verantwoordelijk voor de correcte betaling van de elektronische postzegels en voor eventuele met de PC 50 uitgeoefende fraude. Het is dan aan deze eigenaar om toegang tot het programma voor het aanschaffen van een elektronische postzegel aan autorisatieregels te binden.

In een verdere uitvoeringsvorm met behulp van een PC 50 kan worden gewerkt met een standaard PC zonder SAM 64. In dit geval kan de PC 50 niet op veilige wijze MAC's berekenen. Dan wordt het frankeerkenmerk ofwel centraal in de centrale 34 ofwel in server systeem 70 geproduceerd en naar de PC 50 verstuurd. De PC 50 combineert het ontvangen frankeerkenmerk dan met eventuele andere informatie en drukt deze af op het poststuk 22 met behulp van printer 62. Dan wordt dus niet meer gewerkt met opslag van een saldo voor elektronische zegels op bankpas 18, maar wordt één frankeerkenmerk per keer opgehaald bij de centrale 34. In dit geval vinden betalingen van elektronische postzegels bij voorkeur direct plaats ofwel door het afboeken van een banksaldo van de gebruiker ofwel van bankpas 18 met elektronische beurs. Om eventuele fraude te kunnen bestrijden moet de gebruiker zich dan op unieke wijze identificeren, bijvoorbeeld met zijn giro/banknummer en een bijbehorende PIN. Identificatie vindt dan bij voorkeur nog steeds plaats met bankpas 18 en het controleren van een PIN-code.

Conclusies

1. Werkwijze voor het afdrukken van een frankeerkenmerk (28) op een document (22), omvattende de volgende stappen:

a. het beschikbaar stellen van een unieke bitstring;

b. het vaststellen van een identificatiecode;

c. het beveiligd afdrukken van het frankeerkenmerk (28) op het document (22), welk frankeerkenmerk tenminste informatie met betrekking tot de bitstring en de identificatiecode omvat;

met het kenmerk, dat de bitstring wordt geselecteerd uit een centraal opgeslagen verzameling van unieke bitstrings en centraal wordt geregistreerd welke unieke bitstrings voor gebruik beschikbaar zijn gesteld.

2. Werkwijze volgens conclusie 1 met het kenmerk, dat voorafgaand aan stap c de unieke bitstring en de identificatiecode, beveiligd met behulp van een eerste message authentication code en/of beveiligd door codering, door een terminal (2) op een informatiedrager (18) met geheugen worden opgeslagen en stap c geschiedt na inlezing van de informatiedrager door een afdrukeenheid (20).

3. Werkwijze volgens conclusie 2 met het kenmerk, dat behalve de unieke bitstring en de identificatiecode tevens een terminalidentificatiecode, beveiligd met behulp van de eerste message authentication code en/of door de codering, door de terminal (2) op de informatiedrager (18) met geheugen wordt opgeslagen.

4. Werkwijze volgens conclusie 2 of 3 met het kenmerk, dat na inlezing van de informatiedrager (18) door de afdrukeenheid (20), gebruik van de unieke bitstring voor afdrukken van een verder frankeerkenmerk op een verder document onmogelijk wordt gemaakt door de afdrukeenheid (20).

5. Werkwijze volgens conclusie 2 of 3 met het kenmerk, dat na inlezing van de informatiedrager (18) wordt gecontroleerd of de waarde van een teller op de informatiedrager (18) zich binnen voorafbepaalde grenzen bevindt, en indien dit het geval is de waarde van de teller na het inlezen wordt aangepast en stap c wordt uitgevoerd en indien dit

niet het geval is stap c wordt geblokkeerd.

6. Werkwijze volgens conclusie 1 met het kenmerk, dat bij het uitvoeren van stap c gebruik wordt gemaakt van een computer (50) en een daarop aangesloten afdrukeenheid (62).

7. Werkwijze volgens een van de voorgaande conclusies met het kenmerk, dat de identificatiecode een gebruikersindentificatiecode en/of een afdrukeenheididentificatiecode omvat.

8. Werkwijze volgens een van de voorgaande conclusies met het kenmerk, dat over het frankeerkenmerk een tweede message authentication code wordt berekend en dat ook deze wordt afgedrukt en/of het frankeerkenmerk gecodeerd wordt afgedrukt.

9. Werkwijze volgens een van de voorgaande conclusies met het kenmerk, dat de verzameling unieke bitstrings in een eerste centraal geheugen (38) is opgeslagen, gebruikte combinaties van identificatiecodes en unieke bitstrings in een tweede centraal geheugen (40) worden opgeslagen, op documenten afgedrukte frankeerkenmerken worden ingelezen, in de ingelezen frankeerkenmerken aanwezige combinaties van identificatiecodes en unieke bitstrings in een derde centraal geheugen (42) worden opgeslagen en worden vergeleken met de in het tweede centrale geheugen opgeslagen gebruikte combinaties.

10. Systeem voor het afdrukken van een frankeerkenmerk (28) op een document (22), omvattend:

a. middelen (34) voor het beschikbaar stellen van een unieke bitstring;

b. middelen (4; 52) voor het vaststellen van een identificatiecode;

c. middelen (20; 62) voor het beveiligd afdrukken van het frankeerkenmerk (28) op het document (22), welk frankeerkenmerk tenminste informatie met betrekking tot de bitstring en de identificatiecode omvat;

met het kenmerk, dat de middelen (34) voor het beschikbaar stellen van de unieke bitstring een eerste centraal opgesteld geheugen (38) met een verzameling van unieke bitstrings omvatten, waaruit de unieke

bitstring wordt geselecteerd, en dat middelen zijn voorzien voor het centraal registreren welke unieke bitstrings voor gebruik beschikbaar zijn gesteld.

11. Systeem voor het afdrukken van een frankeerkenmerk (28) volgens conclusie 10 met het kenmerk, dat het systeem een terminal (2) en een afdrukeenheid (20) omvat, welke terminal (2) is ingericht om voorafgaand aan stap c de unieke bitstring tezamen met de identificatiecode, beveiligd met behulp van een eerste message authentication code en/of beveiligd door codering, op een informatiedrager (18) met geheugen op te slaan en de afdrukeenheid (20) is ingericht om stap c uit te voeren na inlezing van de informatiedrager.

12. Systeem volgens conclusie 11 met het kenmerk, dat de terminal is ingericht om een kopie van ofwel de unieke bitstring tezamen met de identificatiecode en de eerste message authentication code ofwel de unieke bitstring en de identificatiecode in gecodeerde vorm naar een centrale (34) te sturen.

13. Systeem volgens conclusie 11 of 12 met het kenmerk, dat de terminal (2) is ingericht om behalve de unieke bitstring en de identificatiecode tevens een terminalidentificatiecode, beveiligd met behulp van de eerste message authentication code en/of beveiligd door codering, op de informatiedrager (18) met geheugen op te slaan.

14. Systeem volgens conclusie 11, 12 of 13 met het kenmerk, dat de afdrukeenheid (20) is ingericht om na inlezing van de informatiedrager (18) gebruik van de unieke bitstring voor afdrukken van een verder frankeerkenmerk op een verder document onmogelijk te maken.

15. Systeem volgens conclusie 11, 12 of 13 met het kenmerk, dat de afdrukeenheid (20) is ingericht om na inlezing van de informatiedrager (18) te controleren of de waarde van een teller op de informatiedrager (18) zich binnen voorafbepaalde grenzen bevindt, en indien dit het geval is stap c uit te voeren en de waarde van de teller na het inlezen aan te passen en indien dit niet het geval is stap c te blokkeren.

16. Systeem volgens conclusie 10 met het kenmerk, dat het een computer (50) omvat en een daarop aangesloten afdrukeenheid (62) voor het uitvoeren van stap c.

17. Systeem volgens conclusie 16 met het kenmerk, dat het systeem is voorzien van op afstand van de computer (50) opgestelde middelen (70) om de unieke bitstring tezamen met de identificatiecode, beveiligd met een eerste message authentication code en/of beveiligd door codering, naar de computer (50) te sturen en een kopie van deze gegevens naar een centrale (34) te sturen.

18. Systeem volgens conclusie 16 met het kenmerk, dat de computer is voorzien van middelen (64) om met behulp van de afdrukeenheid (62) de unieke bitstring tezamen met de identificatiecode, beveiligd met een eerste message authentication code en/of beveiligd door codering op het document af te drukken en optioneel een kopie van deze gegevens naar een centrale (34) te sturen.

19. Systeem volgens een van de conclusies 10 tot en met 18 met het kenmerk, dat de identificatiecode een gebruikersidentificatiecode en/of afdrukeenheididentificatiecode omvat.

20. Systeem volgens een van de conclusies 10 tot en met 19 met het kenmerk, dat het systeem is ingericht om over het frankeerkenmerk een tweede message authentication code te berekenen en af te drukken en/of het frankeerkenmerk gecodeerd af te drukken.

21. Systeem volgens een van de conclusies 10 tot en met 20 met het kenmerk, dat het systeem verder een tweede centraal geheugen (40) voor het opslaan van combinaties van identificatiecodes en verstrekte unieke bitstrings omvat, centrale invoermiddelen (44) voor het invoeren van op documenten afgedrukte frankeerkenmerken, een derde centraal geheugen (42) voor het opslaan van in de ingevoerde frankeerkenmerken aanwezige combinaties van identificatiecodes en unieke bitstrings en met de centrale invoermiddelen en de eerste, tweede, derde centrale geheugens verbonden processormiddelen (36) voor het met elkaar vergelijken van gegevens in de tweede en derde centrale geheugens.

22. Centrale (34) voorzien van een eerste centraal geheugen (38) met een verzameling unieke bitstrings, een tweede centraal geheugen (40) voor het opslaan van combinaties van identificatiecodes en verstrekte unieke bitstrings welke combinaties corresponderen met frankeerkenmerken (28) die op een document (22) zijn afgedrukt, centrale invoermiddelen (44) voor het invoeren van op documenten afgedrukte frankeerkenmerken, een derde centraal geheugen (42) voor het opslaan van in de ingevoerde frankeerkenmerken aanwezige combinaties van identificatiecodes en unieke bitstrings en met de centrale invoermiddelen en de eerste, tweede, derde centrale geheugens verbonden processormiddelen (36) voor het met elkaar vergelijken van gegevens in de tweede en derde centrale geheugens.

23. Middelen voor een apparaat (20; 50), dat is ingericht voor het afdrukken van een frankeerkenmerk op een document (22), welke middelen tenminste zijn ingericht voor het ontvangen van gegevens van een informatiedrager (18), welke gegevens tenminste een unieke, uit een verzameling van unieke bitstrings afkomstige bitstring omvatten, voor het samenstellen en beschikbaar stellen van gegevens voor het frankeerkenmerk (28) voor het document (22) in beveiligde vorm, zodat het apparaat (20; 50) het frankeerkenmerk (28) beveiligd op het document kan afdrukken, welk frankeerkenmerk tenminste de genoemde gegevens alsmede een identificatiecode omvat.

24. Middelen volgens conclusie 23, met het kenmerk, dat deze zijn ingericht om na ontvangst van de gegevens van de informatiedrager (18) te controleren of de waarde van een teller op de informatiedrager (18) zich binnen voorafbepaalde grenzen bevindt, en indien dit het geval is de informatiedrager (18) te instrueren om de waarde van de teller aan te passen en indien dit niet het geval is het afdrukken van het frankeerkenmerk te blokkeren.

25. Informatiedrager (18) voorzien van een geheugen met daarin opgenomen tenminste de volgende gegevens: een unieke, uit een verzameling van unieke bitstrings geselecteerde bitstring, een identificatiecode en een message authentication code die is berekend over tenminste de unieke bitstring en de identificatiecode en/of de unieke bitstring en de identificatiecode in gecodeerde vorm.

26. Door een computer uitleesbare informatiedrager, die is voorzien van software welke na te zijn ingelezen de computer in staat stelt tot het uitvoeren van een werkwijze voor het afdrukken van een frankeerkenmerk (28) op een document (22), omvattende de volgende stappen:

a. het ontvangen van een unieke bitstring;

b. het vaststellen van een identificatiecode;

c. het beveiligd afdrukken van het frankeerkenmerk (28) op het document (22), welk frankeerkenmerk tenminste informatie met betrekking tot de bitstring en de identificatiecode omvat;

waarbij de bitstring wordt ontvangen uit een centraal opgeslagen verzameling van unieke bitstrings.

27. Gegevensdraaggolf voorzien van software voor het downloaden naar een computer, welke na te zijn ingelezen de computer in staat stelt tot het uitvoeren van een werkwijze voor het afdrukken van een frankeerkenmerk (28) op een document (22), omvattende de volgende stappen:

a. het ontvangen van een unieke bitstring;

b. het vaststellen van een identificatiecode;

c. het beveiligd afdrukken van het frankeerkenmerk (28) op het document (22), welk frankeerkenmerk tenminste informatie met betrekking tot de bitstring en de identificatiecode omvat;

waarbij de bitstring wordt ontvangen uit een centraal opgeslagen verzameling van unieke bitstrings.

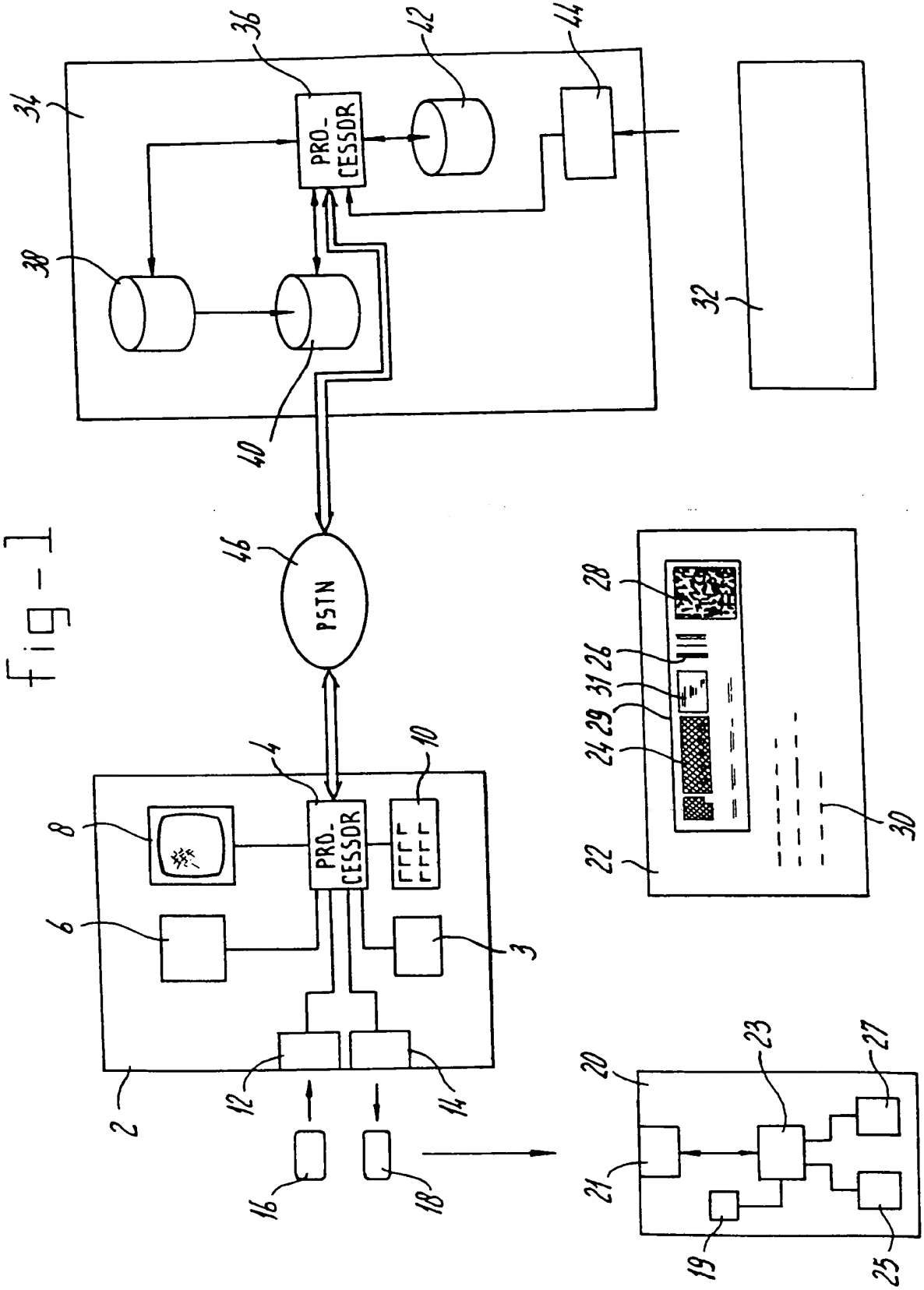
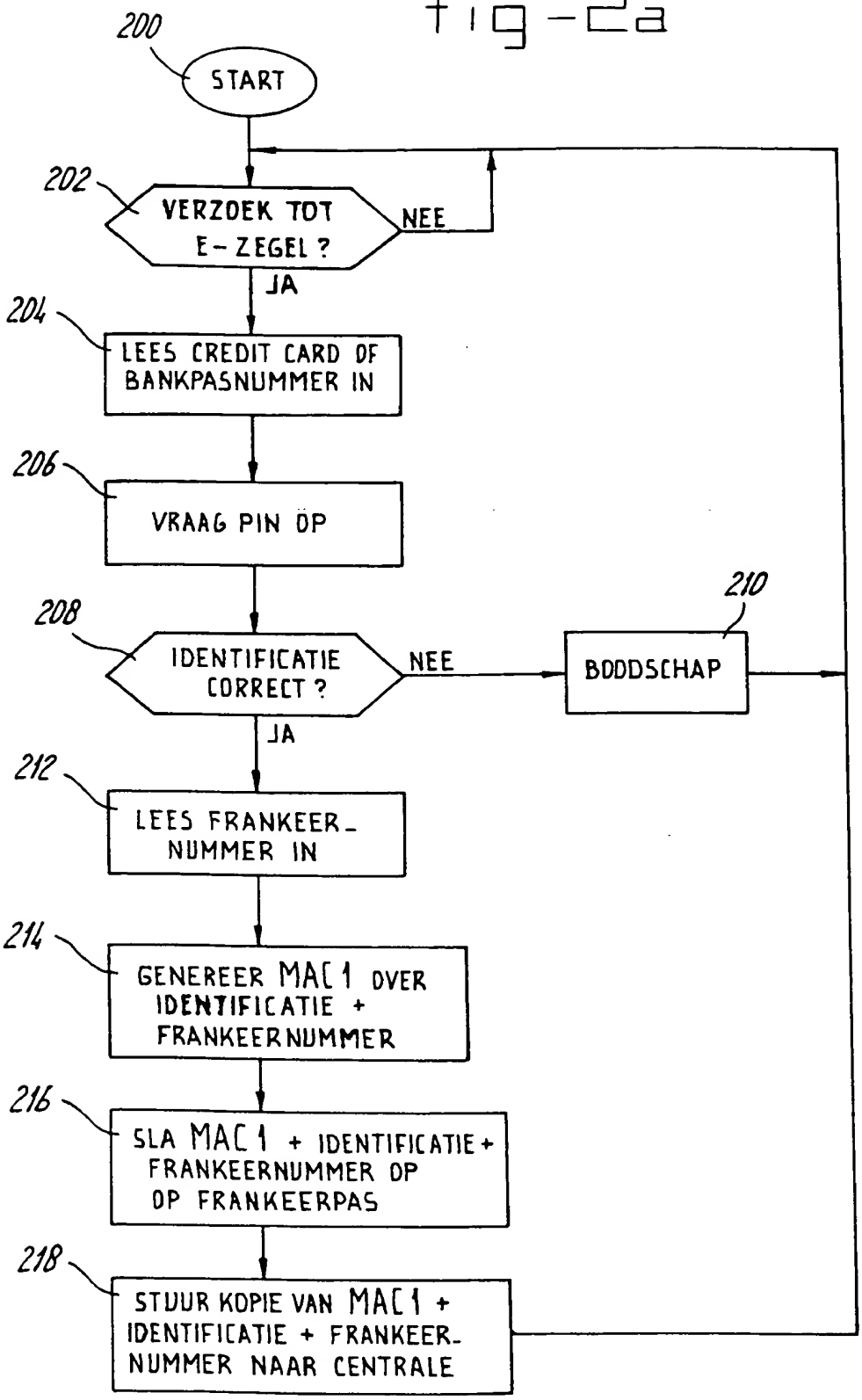

PRO-
CESSOR
PSTN
PRO-
CESSOR
34
36
42
44
38
40
32
46
28
26
31
24
29
22
30
8
6
4
10
3
2
12
14
16
18
20
23
27
21
19
25

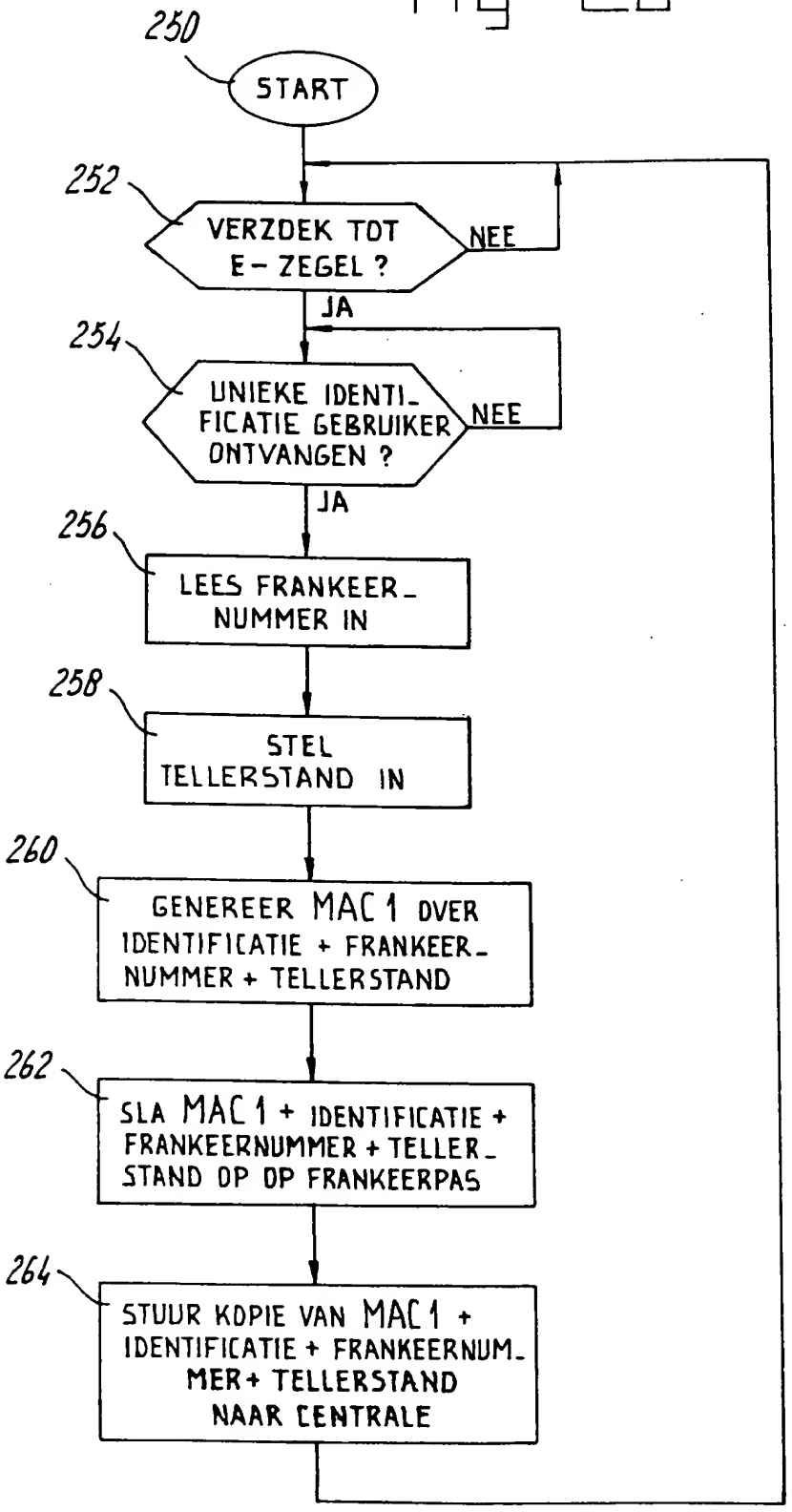
fig-1

fig-2a



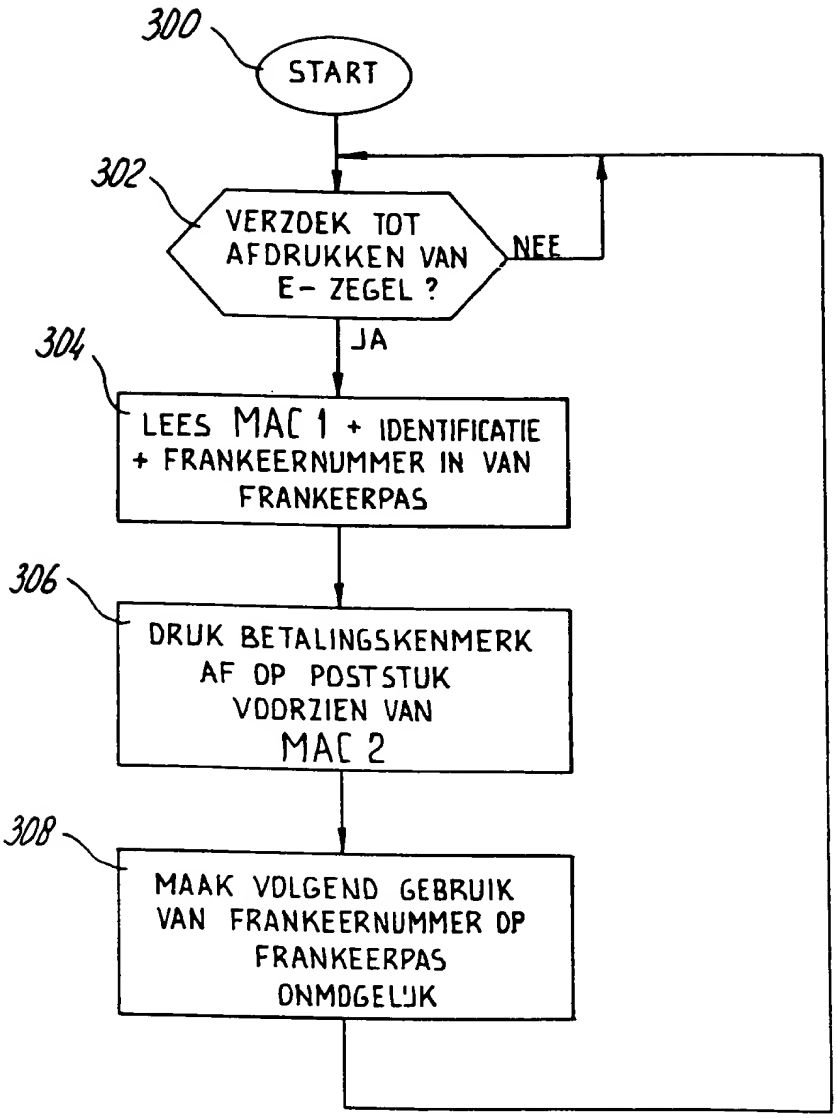
E - ZEGELUITGIFTE

fig-2b



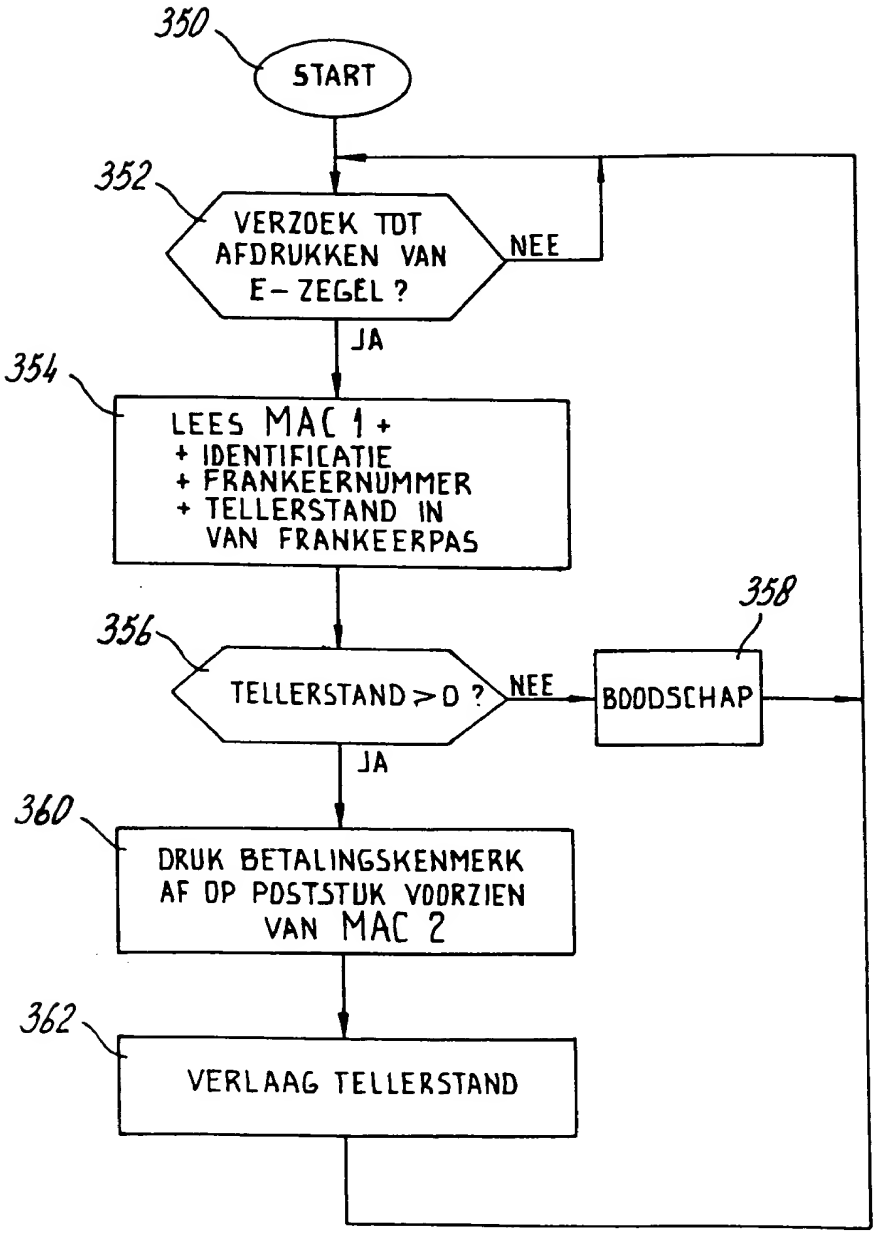
E-ZEGELUITGIFTE MET TELLER

Fig - 3a



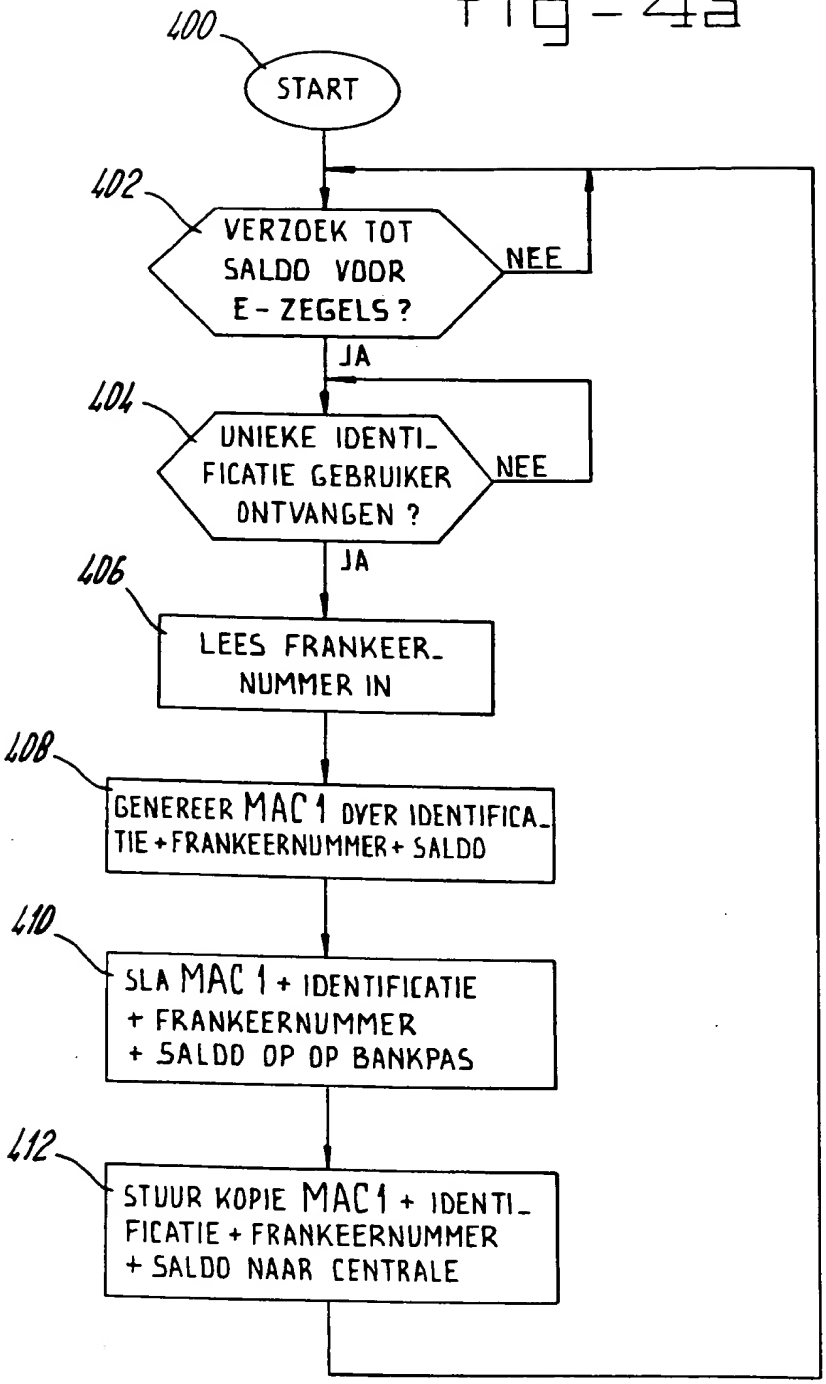
AFDRUKKEN VAN E - ZEGEL

Fig - 3b



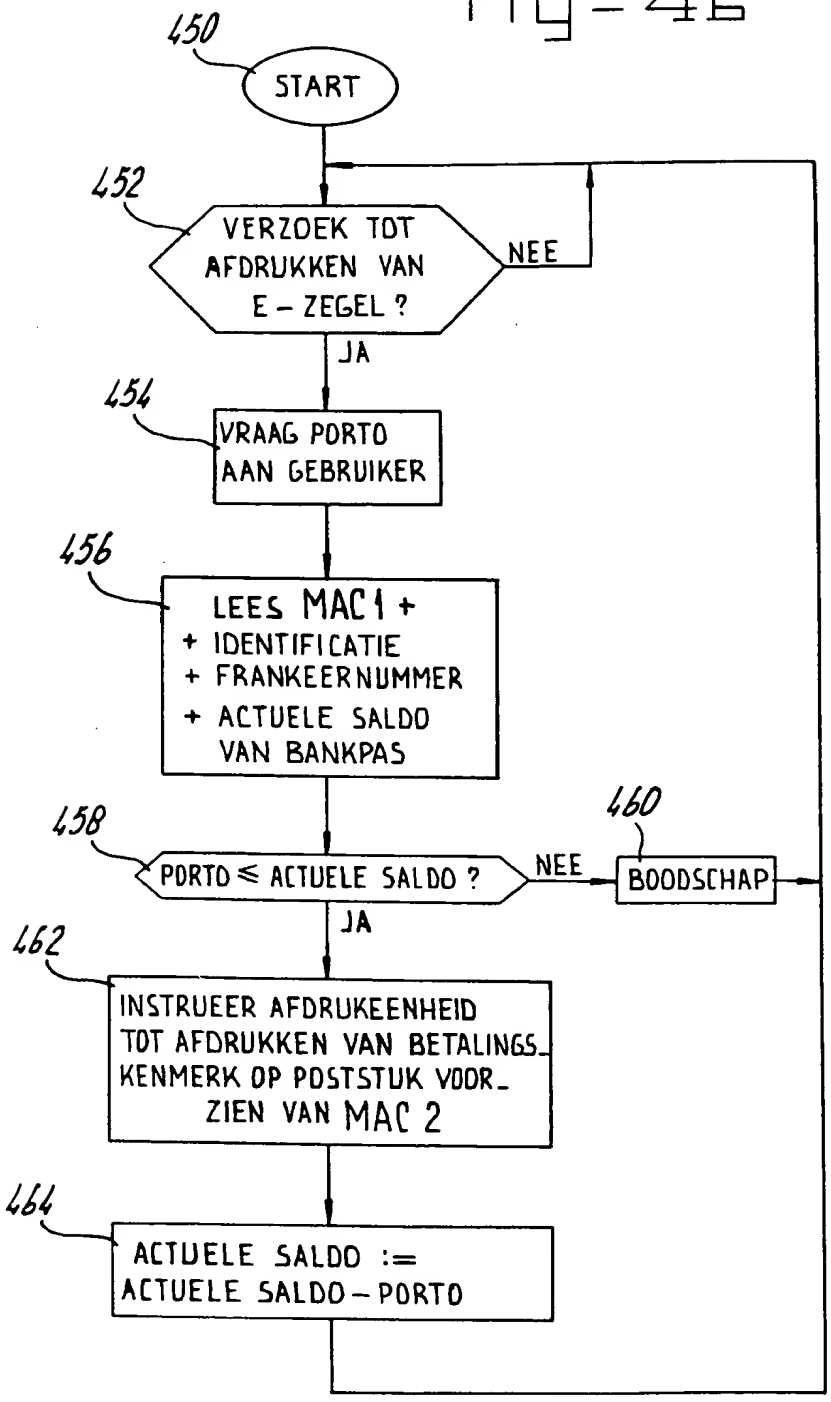
AFDRUKKEN MET TELLER

Fig-4a



E-ZEGEL OPSLAG MET PC-UITVOERINGSVORM

fig-4b



AFDRUKKEN VIA
PC-UITVOERINGSVORM

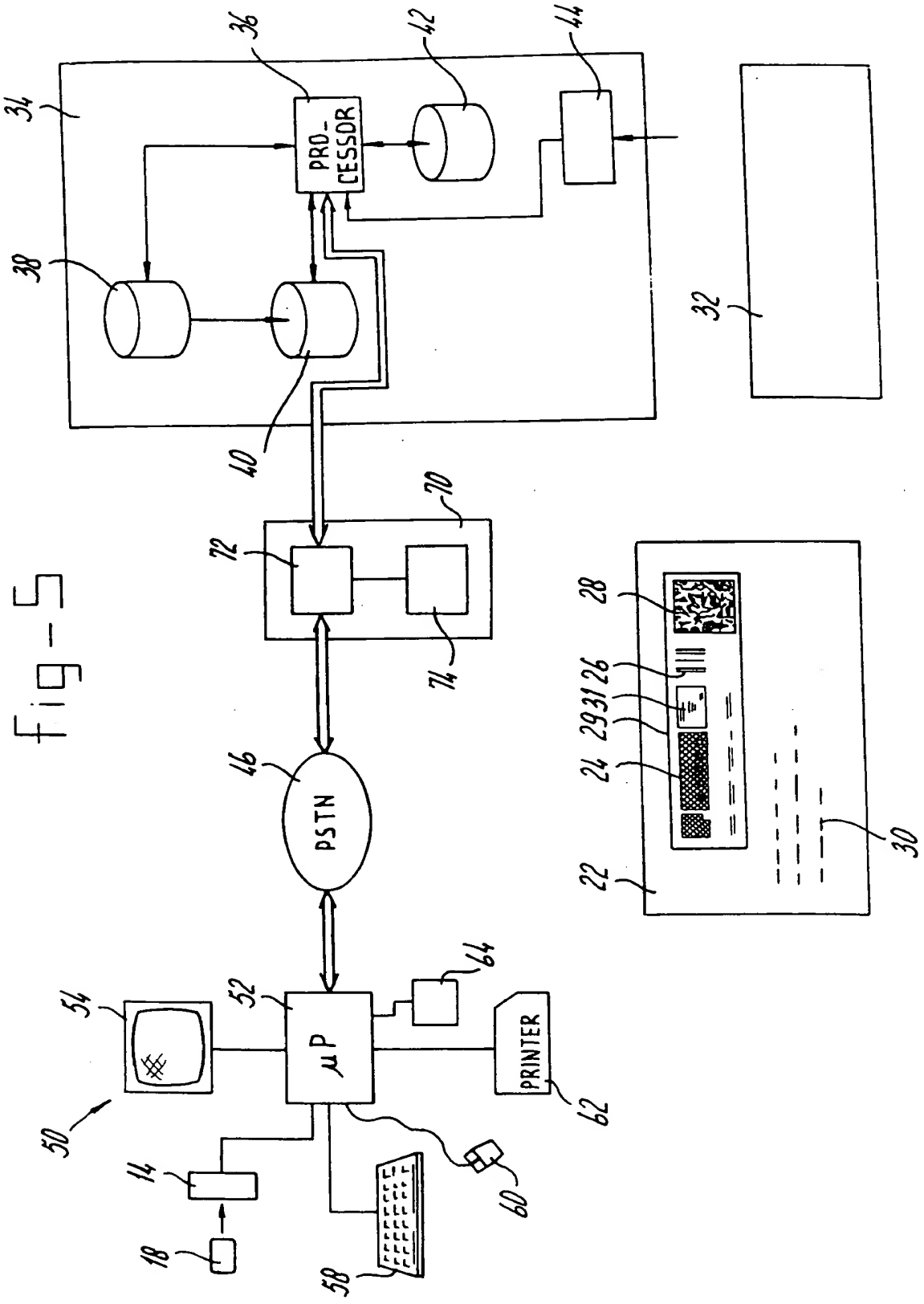

34
36
PRO-
CESSOR
42
44
38
40
32
70
72
74
46
PSTN
28
26
29
31
24
22
30
54
52
μP
64
PRINTER
62
50
14
18
58
60

Fig-5